#4

PTO-1449

Information Disclosure Citation in an Application

Application No	Applicant(s)		
09/668,027	William T. Jennings		
Docket Number	**Group Art Unit**	**Filing Date**	
064751.0315	2131	September 21, 2000	

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE
MV	A	5,073,870	12/17/91	Morita	364	746	01/29/90
	B	5,101,431	03/31/92	Even	380	30	12/14/90
	C	5,764,772	06/09/98	Kaufman, et al	380	30	12/15/95
	D	5,815,573	09/29/98	Johnson, et al	380	21	04/10/96
	E	6,061,706	05/09/00	Gai, et al	708	491	10/10/97
	F						
	G						
	H						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
	I							
	J							
	K							

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
MV	L	Choi, Sung-Wook, and Woo, Chong-Ho, *"Bit-Level 1-Dimensional Systolic Modular Multiplication"*, Journal of the Korean Institute of Telematics and Electronics, Sept. 1996, Korea Inst. Telematics & Electron, South Korea, vol. 33B, no. 9, pp. 62-69, XP000619886	09/1996
	M	Blum, Thomas, et al, *"Montgomery Modular Exponentiation on Reconfigurable Hardware"*, Proceedings 14th IEEE Symposium on Computer Arithmetic, Adelaide, AU, April 14-16, 1999, Los Alamitos, CA, pp. 70-77, XP-000876409	04/14/99
	N	Kornerup, Peter, *"A Systolic, Linear-Array Multiplier for a Class of Right-Shift Algorithms"*, IEEE Transactions on Computers, IEEE, Inc., New York, vol. 43, no. 8, 1 August 1994, pp. 892-898	08/1994
	O	Chen, Po-Song, et al, *"A Systolic RSA Public Key Cryptosystem"*, IEEE International Symposium on Circuits and Systems (ISCAS), US, New York, 1996, pp. 408-411, XP000619797	1996
	P	Ciminiera, Luigi, *"Pipelined Arrays for Modular Multiplication"*, IEEE, Monterey, CA, May 31-June 3, 1998, pp. 397-400, XP000873523	05/31/98
	Q	PCT Written Opinion Dated 05 September 2001 for PCT/US00/26073 filed 22 September 2000	09/05/01
	R	PCT International Search Report dated 29 August 2001 for PCT/US01/26073 filed 22 September 2000	08/29/01
	S		

EXAMINER	DATE CONSIDERED
Michael Vaught	4-20-04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

PTO-1449

Information Disclosure Citation in an Application

Application No	Applicant(s)
09/668,027	William T. Jennings

Docket Number	Group Art Unit	Filing Date
064751.0315	2131	September 21, 2000

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE
	A						
	B						
	C						
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						
	L						
	M						
	N						
	O						
	P						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
MV	Q	WO 99/27677	06/03/99	WO	H04L	9/00	X	
	R							
	S							
	T							
	U							
	V							

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
MV	W	PCT Invitation to Pay Additional Fees, dated 03/20/01 for PCT/US00/26073 filed 09/22/00, 4 pages	03/20/01
	X		

EXAMINER	DATE CONSIDERED
Michael Chapman	4-20-04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

PTO-1449

Information Disclosure Citation in an Application

Application No	Applicant(s)		
09/668,027	William T. Jennings		
Docket Number	**Group Art Unit**	**Filing Date**	
064751.0315	2131	September 21, 2000	

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
MV	A	Blase, Matt, et al, *"The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption"*, Presentation at the 1998 RSA Data Security Conference, January 1998, San Francisco, CA, 21 pages	01/1998
	B	Abelson, Hal, et al, *"The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption"*, 27 May 1997 (report on-line, accessed 18 January 1998), 29 pages	05/27/1997
	C	Merkle, R.C., *Secure Communications Over Insecure Channels,"* Communications of the ACM, April 1978, Vol. 21, No. 4, pages 294-299	1976
	D	Barlow, J.P., *"A Plain Text on Crypto Policy"*, Communications of the ACM, Vol. 36, No. 11, November 1993, pages 21-26	11/1993
	E	Holleyman, Robert W. *"On the Export of Software with Encryption Capabilities"*, testimony presented at Key Escrow Meeting, National Institute of Standards and Technology, Gaithersburg, MD, September 6, 1995, pages 1-7	09/06/1995
	F	Cover Page and LOC publication information page (2 pgs) for: Schwartau, Winn, *"Information Warfare: Chaos on the Electronic Superhighway", Thunder's Mouth Press, New York, 1994, LOC No. QA76.9.A25S354, containing 432 pgs.*	1994
	G	Staniford-Chen, Heberlein, L. Todd, *"Holding Intruders Accountable on the Internet"*, Proceedings of the 1995 IEEE Symposium on Security and Privacy, May 8-10, 1995, Oakland, CA, pages 39-49	05/08/1995
	H	Walker, S.T., et al, *"Commercial Key Escrow: Something for Everyone Now and for the Future"*, Trusted Information Systems, Inc., Report #541, January 3, 1995, 10 pages	01/03/1995
	I	Arneke, David, *"Clipper Chip Technology"*, AT&T Media Relations/Marketing Communications, May 1993, 21 pages	05/93
	J	Madsen, Wayne, *"Information Warfare: Indications and Warnings"*, Conference Proceedings, 19th National Information Systems Security Conference, Baltimore, MD, October 22-25, 1996, pages 726-736	10/22/1996
	K	Denning, Dorothy E., *"Descriptions of Key Escrow Systems"*, unpublished, http:/www.cosc.georgetown.edu/~denning/crypto /Appendix html, February 26, 1997, 38 pages	02/26/1997
	L	Cover Page and LOC publication information page (2 pgs) for: Aho, Alfred, *"Currents in the Theory of Computing"*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1973, LOC No. QA267.5.S4A33, containing 245 pages	1973
MV	M	Orup, Holger, *"Simplifying Quotient Determination in High-Radix Modular Multiplication"*, Proceedings of the 12th Symposium on Computer Arithmetic, July 19-21, 1995, Bath, England, sponsored by the IEEE Computer Society Technical Committee on VLSI, pages 193-199	07/19/1995

EXAMINER	DATE CONSIDERED
Michael Vaughn	4-20-04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

PTO-1449

Information Disclosure Citation in an Application

Application No	Applicant(s)		
09/668,027	William T. Jennings		
Docket Number	**Group Art Unit**	**Filing Date**	
064751.0315	2131	September 21, 2000	

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
	N	Jennings, William T., Dunham, James G., *"Key Escrowing Systems and Limited One Way Functions"*, Conference Proceedings, Vol. I, 19th National Information Systems Security Conference, Baltimore, MD, October 22-25, 1996, 11 pages	10/22/1996
	O	Higgins, John C., *"Evaluating the Strength of Ciphers"*, National Institute of Standards and Technology/National Computer Security Center, 18th National Information Systems Security Conference, Baltimore, MD, October 10-13, 1995, pages 395-403	10/10/1995
	P	Alves-Foss, Jim, *"The Use of Belief Logics in the Presence of Causal Consistency Attacks"*, Conference Proceedings, 20th National Information Systems Security Conference, Baltimore, MD, October 1997, 12 pages	10/1997
	Q	Burrows, Michael, et al, *"A Logic of Authentication"*, Association for Computing Machinery, Transactions on Computer Systems, February 1990, Vol. 8, No. 1, pages 18-36	02/1990
	R	Rivest, R. L., et al, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*, Communications of the ACM, February 1978, Vol. 21, No. 2, pages 120-126	02/1978
	S	Cover Page and LOC publication information page (2 pgs) for: Welsh, Dominic, *"Codes and Cryptography"*, Oxford University Press, Oxford, UK, 1988, LOC No. Z103.W46, containing 257 pages	1998
	T	Rabin, Michael O., *"Digitalized Signatures and Public-Key Functions As Intractable as Factorization"*, MIT Laboratory for Computer Science, TR-212, January 1979, pages 1-16	01/1979
	U	Montgomery, Peter L., *"Modular Multiplication Without Trial Division"*, Mathematics of Computation, American Mathematical Society, Providence, RI, April 1985, Vol. 44, No. 170, pages 519-521	04/1985
	V	Cover Page and LOC publication information page (2 pgs) for: Soderstrand, Michael A., et al, *"Residue Number System Arithmetic: Modern Applications in Digital Signal Processing"*, IEEE Press, 1986, LOC No. QA247.35.R45	1986
	W	Di Claudio, Elio D., Piazza, Francesco, *"Fast Combinatorial RNS Processors for DSP Applications"*, IEEE Transactions on Computers, May 1995, Vol. 44, No. 5, pages 624-633	05/1995
	X	Alia, Giuseppe, Martinelli, Enrico, *"A VLSI Modulo m Multiplier"*, IEEE Transactions on Computers, July 1991, Vol. 40, No. 7, pages 873-878	07/1991
	Y	Paliouras, V., et al, *"Systematic Derivation of the Processing Element of a Systolic Array Based on Residue Number System"*, 1992 IEEE International Symposium on Circuits and Systems, May 10-13, 1992, San Diego, CA, Vol. 2 of 6, pages 815-818	05/10/92
	Z	Parhami, Behrooz,, Hsun-Feng Lai, *"Alternate Memory Compression Schemes for Modular Multiplication"*, IEEE Transactions on Signal Processing, March 1993, Vol. 41, No. 3, pages 1378-1385	03/1993
	AA	Walter, Colin D., *"Systolic Modular Multiplication"*, IEEE Transactions on Computers, March 1993, Vol. 42, No. 3, pages 376-378	03/1983

EXAMINER	DATE CONSIDERED
Michael Vaught	4-20-04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

PTO-1449 **Information Disclosure Citation in an Application**	Application No 09/668,027	Applicant(s) William T. Jennings	
	Docket Number 064751.0315	Group Art Unit 2131	Filing Date September 21, 2000

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
MV	BB	Eldridge, Stephen E., Walter, Colin D., *"Hardware Implementation of Montgomery's Modular Multiplication Algorithm"*, IEEE Transactions on Computers, June 1993, Vol. 42, No. 6, pages 693-699	06/1993
	CC	Koc, Cetin Kaya, et al, *"Analyzing and Comparing Montgomery Multiplication Algorithms"*, IEEE Micro, June 1996, Vol. 16, No. 3, pages 26-33	06/1996
	DD	Kornerup, Peter, *"High-Radix Modular Multiplication for Cryptosystems"*, Proceedings, IEEE 11th Symposium on Computer Arithmetic, June 29-July 2, 1993, Windsor, Ontario, pages 277-283	06/29/1993
	EE	Takagi, Naofumi, *"A Modular Multiplication Algorithm with Triangle Additions"*, Proceedings, IEEE 11th Symposium on Computer Arithmetic, June 29-July 2, 1993, Windsor, Ontario, pages 272-276	06/29/1993
	FF	Jennings, W. T., Dunham, J.G., *"Multistage Algorithm for Limited One-Way Functions"*, presented at the 20th National Information Systems Security Conference, Baltimore, MD, October 1997, 12 pages	10/1997
	GG	Naccache, David, M'Raihi, David, *"Cryptographic Smart Cards"*, IEEE Micro, June 1996, Vol. 16, No. 3, pages 14-24	06/1996
	HH	Dhem, Jean-Francois, et al, *"SCALPS: Smart Card for Limited Payment Systems"*, IEEE Micro, June 1996, Vol. 16, No. 3, pages 42-51	06/1996
	II	Levin, Leonid A., *"Average Case Complete Problems"*, SIAM Journal on Computing, February 1986, Vol. 15, No. 1, pages 285-286	02/1986
	JJ	Ben-David, Shai, et al, *"On the Theory of Average Case Complexity"*, Journal of Computer and System Sciences, April 1992, Vol. 44, No. 2, pages 193-219	04/1992
	KK	Schuler, Rainer, Watanabe, Osamu, *"Towards Average-Case Complexity Analysis of NP Optimization Problems"*, Proceedings, IEEE Tenth Annual Structure in Complexity Theory Conference, Minneapolis, MN, June 19-22, 1995, pages 148-159	06/19/1995
	LL	Gurevich, Yuri, *"Average Case Completeness"*, Journal of Computer and System Sciences, June 1991, Vol. 42, No. 3, pages 346-398	06/1991
✓	MM	Cover Page and LOC publication information page (2 pgs) for: Schneier, Bruce, *"Applied Cryptography, Protocols, Algorithms, and Source Code in C"*, Associate Publishers, 1993, LOC No. QA76.9.A25S35, containing 618 pages	1993
	NN		
	OO		
	PP		
	QQ		
	RR		
	SS		

EXAMINER Michael Vaughn	DATE CONSIDERED 4-20-04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.